IN THE CLAIMS

Please amend the claims as follows:

Claim 1 (Currently Amended): An encryption device for encrypting information on a unique confidential target, comprising:

an imaging unit configured to perform imaging on a target and to output analog first and second signals, the first signal including image data of an inside portion of the unique confidential target, and the second signal including uniform image data of a uniform imaging target to create variation patterns ~~specific~~ unique to the imaging unit;

an identification unit configured to perform analog/digital conversion on the first signal having the image data of the inside portion of the unique confidential target to create identification information;

a creation unit configured to perform analog/digital conversion on the second signal having the variation patterns unique to the imaging unit by performing an algorithm on the second signal to create encryption key information ~~unique to the imaging unit~~; and

an encryption unit configured to encrypt the identification information by using the encryption key information.

Claim 2 (Currently Amended): The encryption device according to claim 1, wherein the creation unit includes a storage unit configured to store a plurality of predetermined evaluation patterns having different hamming distances between higher-ranked uniform image data and a prescribed evaluation pattern data, and the creation unit is further configured to create the encryption key information by using at least one calculated hamming distance of the image data of the first signal and the plurality of predetermined evaluation patterns.

Claim 3 (Previously Presented): The encryption device according to claim 2, further comprising:

a communication unit configured to communicate with a prescribed communication party; and

the creation unit is further configured to select evaluation patterns requested by the communication party, from the plurality of predetermined evaluation patterns stored in the storage unit.

Claims 4 and 5 (Canceled).

Claim 6 (Currently Amended): An encryption method for encrypting information on a unique confidential target, comprising:

performing imaging on an inside portion of a target via an imaging unit;

outputting an analog first signal that includes image data of the inside portion of the unique confidential target;

outputting an analog second signal that includes uniform image data of a uniform imaging target to create variation patterns ~~specific~~ unique to the imaging unit;

performing analog/digital conversion on the first signal having the image data of the inside portion of the unique confidential target to create identification information;

performing analog/digital conversion on the second signal having the variation patterns unique to the imaging unit to create encryption key information by performing an algorithm on the second signal ~~unique to the imaging unit~~; and

encrypting via a processor the identification information by using the encryption key information.

Claim 7 (Currently Amended): The encryption method according to claim 6, further comprising:

storing a plurality of predetermined evaluation patterns having different hamming distances between higher-ranked uniform image data and a prescribed evaluation pattern data; and

creating the encryption key information including calculating at least one hamming distance of the image data of the first signal and the plurality of predetermined evaluation patterns.

Claim 8 (Previously Presented): The encryption method according to claim 7, further comprising:

selecting evaluation patterns requested by a prescribed communication party, from the plurality of predetermined evaluation patterns being stored.

Claims 9 and 10 (Canceled).

Claim 11 (Currently Amended): An encryption device for encrypting information on a unique confidential target, comprising:

imaging means for performing imaging on a target and outputting analog first and second signals, the first signal including image data of an inside portion of the unique confidential target, and the second signal including uniform data of a uniform imaging target to create variation patterns ~~specific~~ unique to the imaging means;

identification means for performing analog/digital conversion on the first signal having the image data of the inside portion of the unique confidential target to create identification information;

creation means for performing analog/digital conversion on the second signal having the variation patterns unique to the imaging means to create encryption key information by performing an algorithm on the second signal ~~unique to the imaging means~~; and

encryption means for encrypting the identification information by using the encryption key information.

Claim 12 (Previously Presented): The encryption device according to claim 1, wherein the imaging unit is further configured to project near-infrared light into the target.

Claim 13 (Previously Presented): The encryption device according to claim 1, wherein the first signal includes blood vessel pattern information representing a formation pattern of blood vessel tissues inside the target.

Claim 14 (Previously Presented): The encryption device according to claim 1, wherein the second signal includes data based on a signal output from a plurality of piezoelectric elements of a touch pad.

Claim 15 (Previously Presented): The encryption device according to claim 1, wherein the second signal includes data based on a signal output from a group of active elements.

Claim 16 (Previously Presented): The encryption device according to claim 1, wherein the second signal includes data based on a signal output from a group of passive elements.